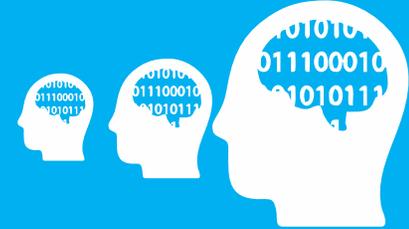# WEB APPLICATION SECURITY

Web application security testing is critical to protecting both your web application system and your organisation. Your web applications sometimes become the #1 attack vector for malicious individuals seeking to breach your company and your business. Available to users 24/7, web apps are the easiest target for criminals seeking access to confidential data of your business.

Our security tests are carried out by employing the same techniques as an attacker located outside your organisation or company and will verify if your web application or web application's server is able to resist hostile attacks and find out whether there are any identified vulnerabilities that can lead to further intrusion and exploitation.

Our team consists of highly skilled and experienced team members with over 10 years of experience in information security and penetration testing, which will help your company to run the business securely with peace of mind and without any worry about being terrorised by hacker attack.

Security tests are conducted using different testing frameworks which are widely used by industries such as Open Web Application Security Project (OWASP), Penetration Testing Executive Standards (PTES), Open Source Security Testing Methodology (OSSTM) and also NIST SP 800-15.

AUTH SCURE

METHODOLOGY WEB APPLICATION SECURITY TESTING

At Authscure, our application penetration testing process targets the entire range of vulnerabilities in your web app. Using the same techniques as sophisticated hackers, we provide unique visibility into security risks that automated tools often miss. To ensure high quality and repeatable engagements, our penetration testing methodology will follow these steps:

Recon

As with malicious hackers, each penetration test begins with information gathering. We will collect all information related to the system, and use all the information to identify or search any vulnerabilities within the system.

Vulnerability Assessment

Once the target has been fully enumerated, we will use both vulnerability scanning tools and manual analysis to identify security flaws. With decades of experience and custom-built tools, our security engineers find weaknesses that most automated scanners miss.

Attack & Post-Exploitation (Proof-Of-Concept)

At this stage of assessment, our consultants review all previous data to identify and safely exploit identified application vulnerabilities. Once sensitive access has been obtained, focus turns to escalation and movement to identify technical risk and total business impact.

During each phase of the compromise, we keep clients and stakeholders informed of testing progress, thus ensuring asset safety and stability.

Mitigation Recommendation

Once the engagement is completed, we will deliver a detailed analysis and threat report, including remediation steps. Our consultants set an industry standard for clear and concise reports, prioritising the highest risk vulnerabilities.

www.authscure.com.my